IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Claims 1-27 (cancel)

28. (New) A system for sending and validating documents using authentication codes and portable verifier elements which can process and store information and which offer a high level of protection against unauthorized readers and writers, the system comprising:

an authentication code for a particular portable verifier device;

a portable verifier device to receive the document authentication code;

at least one portable verifier device operator to encrypt the document to be decrypted by the portable verifier device;

at least one key loaded into the portable verifier device;

a document portal to select and/or purchase the document;

a reader/verifier/recorder to read the document authentication code, transmit it to the portable verifier device, receive the response, decrypts a reader operator using the corresponding code, and validates or rejects the document;

wherein the reader operator encrypts the document using the key of the group of readers/verifiers/recorders in charge of validating the document;

wherein the authentication code is indicated directly or indirectly by a person requesting the document;

wherein no data record of any type is required in the portable verifier device up to the point at which the document is validated;

wherein the portable verifier device is actively involved in the validation; and

wherein the portable verifier device contains a stored list of validated documents such that it is possible to determine, at least, whether or not this is a first validation.

29. (New) The system according to claim 28 wherein the portable verifier device is individualized by the sender using one or more keys of the portable verifier device;

wherein the document is generated from a document portal and the data considered relevant is coded using the key that corresponds to the group of readers/verifiers/recorders involved in the validation of the document, so that the first cryptographic operation can be carried out.

wherein a second cryptographic operation is linked to the first cryptographic operation and includes the key corresponding to the portable verifier device associated with the document,

wherein an authentication code is created for the document and is incorporated therein as a result of these cryptographic operations;

wherein the document is checked by the reader and its authentication code and a third cryptographic operation is carried out to verify those already employed to generate the document;

wherein the portable verifier contains a list of validated documents such that it is possible to determine whether or not this is the first validation.

30. (New) The system according to claim 29 wherein the individualization phase of the portable verifier devices is carried out by storing one or more portable verifier device keys, which must be an symmetric or secret key encryption algorithm;

wherein the first and second cryptographic operations are made up of two encryptions using a symmetric cryptographic algorithm, one using the key of the group of readers/verifiers/recorders involved in the validation of the document and the other using the key that corresponds to the portable verifier device associated with the document;

wherein the third cryptographic operations includes decrypting, by the portable verifier device using its corresponding key of the document's authentication code and the subsequent decryption, carried out by the aforementioned reader/verifier/recorder and its corresponding code.

31. (New) The system according to claim 28 wherein the portable verifier devices is individualized by storing one or more portable verifier device keys, which must be the secret keys of an asymmetric or public key cryptographic algorithm;

wherein the first and second cryptographic operations are based on public key cryptography which is composed of a digital signature with a secret key, and the readers/verifiers/recorders involved in the validation of the document will know its corresponding public key, and an encryption using the corresponding public key of the portable verifier device associated with the document;

wherein the third cryptographic operations is based on a public key cryptography composed of a decryption using the secret key corresponding to the portable verifier device associated with the document and the verification of the signature, using the corresponding public key stored in the readers/verifiers/recorders.

32. (New) The system according to claim 29 wherein the portable verifier devices is individualized by storing one or more portable verifier device keys, which must be the secret keys of an asymmetric or public key cryptographic algorithm;

wherein the first and second cryptographic operations are based on public key cryptography which is composed of air encryption using the public key of the readers/verifiers/recorders involved in the validation of the document, and an encryption using the corresponding public key of the portable verifier device associated with the document; and

wherein the third cryptographic operations is based on public key cryptography composed of a decryption using the secret key corresponding to the portable verifier device associated with the document and a decryption using the secret key of the readers/verifiers/recorders.

33. (New) The system according to claim 29 wherein the portable verifier devices is individualized by storing one or more portable verifier device keys, which are the public keys of an asymmetric or public key cryptographic algorithm;

wherein the first and second cryptographic operation are based on public key cryptography which includes a digital

signature using the secret key that corresponds to the public key stored in the readers/verifiers/recorders involved in the validation of the document and another digital signature using the secret key corresponding to the appropriate individualization key stored in the portable verifier device associated with the document; and

wherein the third cryptographic operations is based on public key cryptography composed of the verification of the signature by the portable verifier device associated with the document using the appropriate individualization key and a second verification of the signature using the public key of the readers/verifiers/recorder.

34. (New) The system according to claim 29 wherein the portable verifier device is individualized by storing one or more portable verifier device keys, which must be the public keys of an asymmetric or public key cryptographic algorithm;

wherein the first and second cryptographic operations are based on public key cryptography which is composed of an encryption using the public key corresponding to the secret key stored in the readers/verifiers/recorders involved in the validation of the document and a digital signature using the secret key corresponding to the appropriate individualization key stored in the portable verifier device associated with the document;

wherein the third cryptographic operations will be based on public key cryptography composed of the verification of the signature by the portable verifier device associated with the document using the appropriate individualization key and a

decryption using the secret key corresponding to the readers/verifiers/recorders.

35. (New) The system according to claim 34 wherein the document is check before the document is validated.

36. (New) The system according to claim 35 wherein the reader/verifier/recorder is informed if the document to be validated in is already included in the list of validated documents so that it can proceed as appropriate.

37. (New) The system according to claim 36 wherein the document to be validated is included in the list of validated documents, provided it was not already there, and the corresponding cryptographic operation will he carried out when reversing, and/or checking the cryptographic operation corresponding to the portable verifier device, and the result is sent to the reader/verifier/recorder so that it can proceed as appropriate.

38. (New) The system according to claim 29 wherein the cryptographic authentication established between the portable verifier device and the reader/verifier/recorder is mutual and firm.

39. (New) The system according to claim 38 wherein a cooperative and random session key is established between the portable verifier device and the reader/verifier/recorder and is used to encrypt the pertinent messages between the two.

40. (New) The system according to claim 28 wherein the portable verifier device is individualized by the senders using one or more keys obtained from the encryption of the serial number with one or more master keys chosen by the portable verifier device operators, so that the master key of each operator and the portable verifier device corresponds to the identifier, which should be legible by the user.

41. (New) The system according to claim 28 wherein the reader/verifier/recorder has been adapted to send information, accepting or rejecting the document and stating the reason why.

42. (New) The system according to claim 28 wherein the reader/verifier/recorder keys are common to the group of readers.

43. (New) The system according to claim 28 wherein the keys stored in the readers/verifiers/recorders are obtained by encrypting the identifiers, or parts of these, using the master keys chosen by the operators.

44. (New) The system according to claim 28 wherein the document has an expiry date, this will be included in the authentication code, so that they can be eliminated from the list of validated documents stored in the portable verifier once this date has passed.

45. (New) The system according to claim 44 wherein the portable verifier device receives the date expired document to be deleted

from the list of validated documents through a digital certificate sent by a competent body.

46. (New) The system according to claim 28 wherein the document and/or authentication code are selected and obtained through internet.

47. (New) The system according to claim 28 wherein the document authentication code is send to the user's mobile telephone.

48. (New) The system according to claim 28 wherein the document's authentication code is send to the user's electronic agenda or any other similar device belonging to the user.

49. (New) The system according to claim 28 wherein the authentication code can be printed through a barcode.

50. (New) The system according to claim 28 wherein the authentication code can be printed through one or more barcodes.

51. (New) The system according to claim 28 wherein the authentication code can be printed through an alphanumerical code.

52. (New) The system according to claim 28 wherein the authentication code can be printed through a dot code.

53. (New) The system according to claim 49 wherein the authentication code can also be printed through an

alphanumerical code so that it can by keyed in manually in the event the automatic reading code deteriorates.

54. (New) The system according to claim 49 wherein the barcodes include the correct reading order.